UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/036,196	12/28/2001	Jingmin He	YOR92001-0553 (8728-537)	2834

			EXAMINER
46069	7590	01/30/2006	FIELDS, COURTNEY D

F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>06 October 2005</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-14</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-14</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-14 are pending.

Response to Arguments

2.   Applicant's arguments filed 06 October 2005 have been fully considered but they
are not persuasive.

3.   Referring to the rejection of claims 1 and 8, the Applicant contends that the prior
art (Newman et al.) does not teach nor disclose a relational database providing a
security dictionary comprising one or more catalogs. The Examiner respectfully
disagrees and asserts that Newman discloses a relational database management
system for internally encrypting non-relational data (See Page 1, Section 0010). Within
the relational database management system, a DBENCRYPT package (security
dictionary) is provided for storing all of the information that is used to manage data
objects within the relational database. (See Page 2, Section 0028) The DBENCRYPT
package comprises one or more catalogs known as DBENCRYPT_KEYS table. The
DBENCRYPT_KEYS table contains two security features in which data can only be
stored within the table based upon an authentication mechanism and the encryption key
used to update information within the table is never stored in the database. Therefore,
the information can never be updated by anyone without authorization through the use
of an authentication mechanism and/or a password. (See Page 3, Section 0032-0035
and Page 4, Sections 0043-0044).

4.   Referring to the rejection of claims 4 and 11, the Applicant contends that the prior

art (Newman et al.) does not teach nor disclose wherein the step of associating the data

with a database column and a user is accomplished with an extended SQL syntax. The

Examiner respectfully disagrees and asserts that Newman discloses encryption of data

associated with a database column by providing the user with row-level encryption

within the tables of the database using SQL syntax as a means for improving data

encryption within a relational database management system. (See Page 1, Sections

004-005)

5.   Referring to the rejection of claims 5 and 12, the Applicant contends that the prior

art (Newman et al.) does not teach nor disclose wherein the working key is provided by

a user. The Examiner respectfully disagrees and asserts that Newman discloses when

the user attempts to access encrypted data, the encrypted data key (working key) for

the current user is retrieved from the DBENCRYPT_KEYS table and is decrypted with

the RSA algorithm using the private key stored in the application context. (See Page 3,

Section 0037)

        6.   Referring to the rejection of claims 7 and 14, the Applicant contends that

the prior art (Newman et al.) does not teach nor disclose receiving a query and private

key from a user checking the ownership of an encrypted column using the security

catalog to verify the user is authorized, internally decrypting the encrypted working

encryption key with the private key, internally decrypting the encrypted column with the

working key, processing the query, and returning an answer to the query to the user.

The Examiner respectfully disagrees and asserts that Newman discloses a SQL syntax

for improving data encryption within a relational database management system. A SQL

is defined as a structure used to query a relational database (See Page 1, Section 004)

The private key from a user is checked for ownership by verifying the user is authorized.

(See Page 4, Section 0071) The working key (encrypted data key) is decrypted with the

private key (See Page 3, Section 0037) An answer is returned to the query to the user

(See Page 4, Sections 0067-0069)

7.   Therefore the rejection of claims 1-14 are maintained in view of the reasons

above and in view of the reasons below.

Claim Rejections - 35 USC § 102

1:      The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 1-14 are rejected under 35 U.S.C. 102(e) as being anticipated by

Newman et al. (Pub No. 2003/0046572).

        Regarding claims 1 and 8, Newman et al. discloses a method and program .

storage of internally encrypting data in a relational database, comprising the steps of:

providing a security dictionary (DBENCRYPT package) comprising one or more

security catalogs (DBENCRYPT_KEYS table) receiving the data from a user

(See page 1, Section 0004 and page 2, Sections 0027-0030)

associating the data with a database column and at least one authorized user,

generating a working encryption key (data key), internally encrypting the working

encryption key using a public key from an authorized user (See page 3, Sections

0031-0034)

storing the encrypted working key in a security catalog and

using the working key to internally encrypt the data (See page 3, Section 0035)

Regarding claims 2 and 9, Newman et al. discloses the claimed limitation

wherein the step of generating a private key needed to decrypt the encrypted working

key (See page 3, Section 0037)

Regarding claims 3 and 10, Newman et al. discloses the claimed limitation

wherein the public key is a password and is used by the system to look up the private

key (See page 3, Sections 0043-0050, page 4, Sections 0051-0059)

Regarding claims 4 and 11, Newman et al. discloses the claimed limitation

wherein the step of associating the data with a database column and a user is

accomplished with an extended SQL syntax and further comprises the step of creating a

relational database object comprising:

the identity of the authorized user, (See page 4, Section 0064-0066)

a relational database table, (See page, Section 0067)

the identity of column within the relational database table, and (See page 4, Section 0069)

one or more security flags the flags indicating user privileges to access the data (See page 4, Sections 0070-0071)

Regarding claims 5 and 12, Newman et al. discloses the claimed limitation wherein the working key is provided by the user (See page 3, Sections 0035-0036)

Regarding claims 6 and 13, Newman et al. discloses the claimed limitation wherein the working key is randomly generated (See page 2, Section 0019, page 3, Section 0034)

Regarding claims 7 and 14, Newman et al. discloses the claimed limitation wherein the steps of:

receiving a query and private key from a user,

checking the ownership of an encrypted column using the security catalog to verify the user is authorized,

internally decrypting the encrypted working encryption key with the private key,

internally decrypting the encrypted column with the working key,

processing the query, and

returning an answer to the query to the user (See page 4, Sections 0072-0080, page 5, Sections 0081-0089)

Conclusion

3.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Courtney D. Fields whose telephone number is 571-

272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off

every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

cdf

January 22, 2006

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137